09 - 19 - 06

TOM

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

OIPE IAP74 SEP 18 2006 PATENT & TRADEMARK OFFICE

PATENT APPLICATION

ATTORNEY DOCKET NO. 10016862-1

IN THE
UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s):	Richard P. Tarquini et al.	Confirmation No.:	4734
Application No.:	10/003,815	Examiner:	B. S. Hoffman
Filing Date:	October 31, 2001	Group Art Unit:	2136

Title: METHOD, COMPUTER-READABLE MEDIUM, AND NODE FOR DETECTING EXPLOITS BASED ON AN INBOUND SIGNATURE OF THE EXPLOIT AND AN OUTBOUND SIGNATURE IN RESPONSE THERETO

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on August 14, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

☐ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

☐ 1st Month $120	☐ 2nd Month $450	☐ 3rd Month $1020	☐ 4th Month $1590

☐ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

☒ I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage, as Express Mail Label No.

EV 568240731US

in an envelope addressed to: MS Appeal Brief - Patents, Commissioner for Patents, Alexandria, VA 22313-1450.

Date of Deposit: September 18, 2006

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

Richard P. Tarquini et al.

By _____

Jody C. Bishop

Attorney/Agent for Applicant(s)

Reg No. : 44,034

Date : September 18, 2006

Telephone : (214) 855-8007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Docket No.: 10016862-1
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Richard P. Tarquini et al.

Application No.: 10/003,815 | Confirmation No.: 4734

Filed: October 31, 2001 | Art Unit: 2136

For: METHOD, COMPUTER-READABLE MEDIUM, AND NODE FOR DETECTING EXPLOITS BASED ON AN INBOUND SIGNATURE OF THE EXPLOIT AND AN OUTBOUND SIGNATURE IN RESPONSE THERETO | Examiner: B. S. Hoffman

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

As required under § 41.37(a), this brief is filed within two months of the Notice of Appeal filed in this case on August 14, 2006, and is in furtherance of said Notice of Appeal.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1206:

I.	Real Party In Interest
II	Related Appeals and Interferences
III.	Status of Claims
IV.	Status of Amendments
V.	Summary of Claimed Subject Matter
VI.	Grounds of Rejection to be Reviewed on Appeal

VII. Argument
VIII. Claims Appendix
IX. Evidence Appendix
X. Related Proceedings Appendix

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is:

Hewlett-Packard Development Company, L.P., a Limited Partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249, Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

II. RELATED APPEALS, INTERFERENCES, AND JUDICIAL PROCEEDINGS

Appellant respectfully notes that copending Application No. 10/002,697 (hereinafter "the '697 application"), which is referenced as a related application in the present application, is on appeal before the Board. The same references are applied in rejecting the claims of the '697 application, and thus the issues raised in the '697 may be affected or have a bearing on the Board's decision in this appeal. A notice of appeal to the Board was filed for the '697 application on June 6, 2006. The Board has not yet rendered a decision on the appeal of the '697 application.

There are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 22 claims pending in application.

B. Current Status of Claims

1. Claims canceled: None

2. Claims withdrawn from consideration but not canceled: None

3. Claims pending: 1-22

4. Claims allowed: None

5. Claims rejected: 1-22

C. Claims On Appeal

The claims on appeal are claims 1-22

IV. STATUS OF AMENDMENTS

A Final Office Action rejecting the claims of the present application was mailed June 14, 2006. In response, Applicant did not file an Amendment After Final Rejection, but instead filed a Notice of Appeal (on August 14, 2006), which this brief supports. Accordingly, the claims on appeal are those as rejected in the Final Office Action of June 14, 2006. A complete listing of the claims is provided in the Claims Appendix hereto.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the separately argued claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. It should be noted that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element.

According to one claimed embodiment, such as that of independent claim 1, a method of detecting an intrusion at a node (e.g., node 270 of FIG. 4) of a network comprises reading a first packet received by the node (*see* page 9, lines 6-8 of the specification). The method further comprises determining a first signature of the first packet (*see* page 9, line 8 of the specification), and comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature (*see* page 9, lines 8-10 of the specification). The method further comprises reading a second packet generated by the node

in response to reception of the first packet (*see* page 9, lines 11-12 of the specification). The method further comprises determining a second signature of the second packet (*see* page 9, lines 12-13 of the specification), and comparing the second signature with the signature file further comprising a second machine-readable logic representative of second packet signature (*see* page 9, lines 13-15 of the specification). Further, the method comprises identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic (*see* page 19, lines 1-32, page 22, lines 3-30, and page 25, line 28 – page 26, line 13 of the specification).

In certain embodiments, such as that of dependent claim 3, the method further comprises executing a directive associated with the second machine readable logic upon determining the second signature corresponds with the second machine readable logic (*see* page 22, lines 3-30 of the specification). And, in certain embodiments, such as that of dependent claim 4, executing a directive associated with the second machine readable logic further comprises discarding the second packet (*see* page 22, lines 3-30 of the specification). Further, in certain embodiments, such as that of dependent claim 5, discarding the second packet further comprises discarding the packet at the network layer of the network stack (e.g., network stack 90 of FIG. 3 and/or network stack 90A of FIG. 6) of the node (*see* page 22, lines 3-30 of the specification).

In certain embodiments, such as that of dependent claim 6, reading a second packet generated by the node in response to reception of the first packet further comprises reading a second packet generated by a network stack of an operating system of the node (*see* page 19, line 1 – page 22, line 30 of the specification).

According to another claimed embodiment, such as that of independent claim 7, a computer-readable medium having stored thereon a set of instructions to be executed is provided (*see* page 26, lines 4-13 of the specification). The set of instructions, when executed by a processor (e.g., CPU 272 of FIG. 4), cause the processor to perform a computer method of reading a first packet (*see* page 9, lines 19-20 of the specification); determining a first signature of the first packet (*see* page 9, line 20 of the specification); comparing the first signature with a first instruction set comprising a first set of machine readable logic

representative of a first packet signature (*see* page 9, lines 21-22 of the specification); reading a second packet generated in response to reception of the first packet (*see* page 9, lines 11-12 and 23-24 of the specification); determining a second signature of the second packet (*see* page 9, line 24 of the specification); comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature (*see* page 9, lines 24-26 of the specification); and identifying the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic (*see* page 19, lines 1-32, page 22, lines 3-30, and page 25, line 28 – page 26, line 13 of the specification).

In certain embodiments, such as that of dependent claim 9, the computer-readable medium further comprises an instruction set that, when executed by the processor, causes the processor to perform the computer method of executing, upon determining the second signature corresponds with the second instruction set, a directive comprised of machine-readable instructions, the second instruction set comprising the directive (*see* page 22, lines 3-30 of the specification). And, in certain embodiments, such as that of dependent claim 10, executing a directive comprised of machine-readable instructions further comprises executing a directive that causes the processor to discard the second packet (*see* page 22, lines 3-30 of the specification). Further, in certain embodiments, such as that of dependent claim 11, executing a directive that causes the processor to discard the second packet further comprises discarding a packet at a network layer of a network stack (e.g., network stack 90 of FIG. 3 and/or network stack 90A of FIG. 6, and *see* page 22, lines 3-30 of the specification).

According to another claimed embodiment, such as that of independent claim 14, a node (e.g., node 270 of FIG. 4) of a network operable to detect an intrusion thereof comprises a central processing unit (e.g., CPU 272 of FIG. 4), and a memory module (e.g., elements 274 and/or 276 of FIG. 4) for storing data in machine readable format for retrieval and execution by a central processing unit. The node further comprises an operating system (e.g., operating system 275 of FIG. 4) comprising a network stack (e.g., network stack 90 of FIG. 3 and/or network stack 90A of FIG. 6) comprising a protocol driver (e.g., protocol driver 135 of FIGS. 3, 4, and 6), a media access control driver (e.g., MAC driver 145 of FIGS. 3, 4, and 6) and a network filter service provider (e.g., network filter service provider 140 of FIG. 6) bound to

the protocol driver and the media access control driver, the network filter service provider operable to receive a first packet (*see* page 10, lines 2-3 of the specification) and to determine a first signature of the first packet (*see* page 10, line 3 of the specification) and compare the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature (*see* page 10, lines 3-5 of the specification), the network filter service provider further operable to receive a second packet generated in response to receipt of the first packet (*see* page 9, lines 11-12 and page 10, lines 6-7 of the specification) and to determine a second signature of the second packet (*see* page 10, line 7 of the specification) and compare the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature (*see* page 10, lines 8-9 of the specification), the network filter service provider operable to identify the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic (*see* page 19, lines 1-32, page 22, lines 3-30, and page 25, line 28 – page 26, line 13 of the specification).

In certain embodiments, such as that of dependent claim 15, the processor is operable to execute a directive causing the network filter service provider to discard the second packet (*see* page 22, lines 3-30 of the specification).

According to another claimed embodiment, such at that of independent claim 19, a method of detecting an intrusion at a node (e.g., node 270 of FIG. 4) of a network comprises reading a response packet by the node (*see* page 10, lines 16-17 of the specification), the response packet generated in response to reception of a first packet by the node (*see* page 9, lines 11-12 of the specification). The method further comprises determining a signature of the response packet (*see* page 10, line 17 of the specification), and comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature (*see* page 10, lines 17-19 of the specification). Further, the method comprises identifying the first packet as an intrusion if the signature corresponds with the machine-readable logic (*see* page 19, lines 1-32, page 22, lines 3-30, and page 25, line 28 – page 26, line 13 of the specification).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-22 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,578,147 to Shanklin et al. (hereinafter "*Shanklin*") in view of U.S. Patent No. 6,279,113 to Vaidya (hereinafter "*Vaidya*").

VII. ARGUMENT

Appellant respectfully traverses the outstanding rejections of the pending claims, and requests that the Board reverse the outstanding rejections in light of the remarks contained herein. The claims do not stand or fall together. Instead, Appellant presents separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

A. Rejections Under 35 U.S.C. §103

Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Shanklin* in view of *Vaidya*. For the reasons presented below, Appellant respectfully requests that the Board overturn these rejections.

To establish a prima facie case of obviousness, three basic criteria must be met. *See* M.P.E.P. § 2143. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the applied references must teach or suggest all the claim limitations. Without conceding any other criteria, the applied references fail to teach or suggest all elements of the claims, and insufficient motivation exists for combining the references in the manner applied.

1. Applied References Fail to Teach or Suggest All Claim Elements

Appellant respectfully submits that the applied combination of *Shanklin* and *Vaidya* fails to teach or suggest all elements of claims 1-22.

Independent Claim 1 and Dependent Claims 2-3

Independent claim 1 recites:

> A method of detecting an intrusion at a node of a network, comprising:
> reading a first packet received by the node;
> determining a first signature of the first packet;
> comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature;
> reading a second packet generated by the node in response to reception of the first packet;
> determining a second signature of the second packet;
> comparing the second signature with the signature file further comprising a second machine-readable logic representative of second packet signature; and
> identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic. (Emphasis added).

As discussed below, neither *Shanklin* nor *Vaidya* teach or suggest comparing a first signature determined for a first received packet with first machine readable logic, comparing a second signature determined for a second packet that is generated in response to reception of the first packet with second machine readable logic, and identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic. Indeed, neither *Shanklin* nor *Vaidya* teach or suggest using, in any way, a signature that is determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion.

Shanklin "is directed to a network intrusion detection system that accommodates the higher packet throughput enabled by today's high speed networks." Col. 2, lines 45-47 of *Shanklin*. "Multiple intrusion detection sensors are used at the entry point to the network, specifically, at an 'internetworking device' such as a router or a switch." Col. 2, lines 48-50 of *Shanklin*. Each sensor is identical to the others, and the sensors operate in parallel and "analyze packets to determine if any packet or series of packets has a 'signature' that matches one of a collection of known intrusion signatures." *See* col. 2, lines 62-67 of *Shanklin*. *Shanklin* mentions that its signature analysis may be performed to packet datastreams incoming to a local network and to outgoing traffic. *See* col. 3, lines 4-7 of

Shanklin. However, *Shanklin* fails to provide any teaching or suggestion of using, in any way, a signature that is determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion. Indeed, the Final Office Action concedes that this element is not taught by *Shanklin*, as discussed below.

Vaidya is directed to a network intrusion detection system (IDS) that includes attack signature profiles which are descriptive of characteristics of known network security violations. *See* abstract of *Vaidya*. *Vaidya* explains that:

> A monitoring device monitors network traffic for data addressed to the network objects. Upon detecting a data packet addressed to one of the network objects, packet information is extracted from the data packet. The extracted information is utilized to obtain a set of attached signature profiles corresponding to the network object based on the association data. A virtual processor executes instructions associated with attack signature profiles to determine if the packet is associated with a known network security violation. *See* Abstract of *Vaidya*.

However, like *Shanklin*, *Vaidya* fails to provide any teaching or suggestion of using, in any way, a signature that is determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion.

While *Shanklin* and *Vaidya* use signatures of packets for identifying whether the corresponding packets for which the signatures are determined are intrusions, neither reference provides any teaching or suggestion whatsoever of using a signature determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion.

The Final Office Action concedes that *Shanklin* does not disclose identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic. *See* pages 3 and 6 of the Final Office Action. However, the Final Office Action asserts that *Vaidya* teaches this element. Appellant respectfully disagrees.

The Final Office Action relies upon column 8, lines 15-39 of *Vaidya* as teaching the above element (*see* page 3 of the Final Office Action). Column 8, lines 15-39 of *Vaidya* merely provides:

> A timer/counter based attack signature profile directs the virtual processor 36 to execute instructions associated with a single expression on every data packet associated with a particular application session to determine whether an event has occurred a threshold number of times within a predetermined time interval. For instance, a timer/counter based attack signature profile might direct the virtual processor 36 to execute an instruction associated with the expression "is user Z attempting to access file A?" on every packet associated with a session application Y. The instructions also direct the virtual processor 36 to determine whether the number of attempts user Z makes to access file A exceeds 5 attempts within any 10 minute period. The first packet which the virtual processor 36 recognizes as being associated with an attempt by user Z to access file A causes the virtual processor 36 to activate a timer 37 and to set a counter 35 to one. The timer and counter information are entered into the state cache 44. Each subsequent detection of an attempt by user Z to access file A triggers the virtual processor 36 to access the timer and counter information from the state cache 44 and to determine whether the threshold has been met. If the threshold is met, a network intrusion has been detected and the virtual processor 36 notifies the reaction module 38.

The relied-upon portion of *Vaidya* in no way teaches or suggests identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic. Rather, the cited portion of *Vaidya* merely teaches using a counter and/or timer to determine the number of attempted unauthorized accesses during a given time period. The above teaching of *Vaidya* uses a counter to count attempted accesses (e.g., received packets requesting access to a file) to determine whether a threshold number of attempted unauthorized accesses are detected during a given time period. This does not use a signature determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion.

Vaidya does not teach or suggest using a signature determined for a packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion. For instance, the above-identified teaching of *Vaidya* is directed to evaluating separately received packets requesting access to a file, and does not use packets generated in response to reception of the received packets in identifying whether the received packets

are intrusions. Rather, the above teaching merely attempts to detect an intrusion by detecting a number of separately received packets requesting access to a file during a given time period.

In response to Applicant's arguments presented in the response of April 5, 2006, the Final Office Action alleges:

> Shanklin appears delinquent in that he doesn't identify the first packet as an intrusion if the first signature corresponds to a data value and the second signature corresponds to a second data value. This is merely an intended use of the compared signatures.

In view of this statement in the Final Office Action, it is unclear whether the Examiner is still relying on *Vaidya* as teaching or suggesting the element, or whether the Examiner is relying solely on *Shanklin* and asserting that the element need not be taught or suggested in any applied reference because it recites merely intended use. In either case, the assertion that the element recites intended use is inaccurate, as discussed below, and appears to be raised by the Examiner in attempt to salvage the rejection because the applied references fail, as discussed above, to teach or suggest the element.

Claim 1 recites "identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic". Such identifying in this manner is an expressly recited part of the method. While the comparisons of the first and second signatures with the first and second machine readable logic are used for identifying the first packet as an intrusion, this is not reciting an "intended use", but is instead expressly reciting how the first packet is identified. Thus, this language is not reciting an intended use, but is instead defining the "identifying" step of the claim, which as discussed above is not taught or suggested by the applied references. As such, it is improper for the Examiner to ignore the express recitation of the identifying step. And, when the identifying step as a whole is properly considered, the applied references fail to teach or suggest such element, as discussed above.

In view of the above, neither *Shanklin* nor *Vaidya* teaches or suggests the above-identified element of claim 1, and thus the applied combination of *Shanklin* and *Vaidya* fails to teach or suggest such element. Accordingly, the rejection of claim 1 should be overturned.

Claims 2-3 each depend from independent claim 1, and are thus likewise believed to be allowable at least based on their dependency from claim 1 for the reasons discussed above. Accordingly, Appellant respectfully requests that the rejection of claims 2-3 also be overturned.

Dependent Claim 4

Dependent claim 4 depends indirectly from claim 1, and thus inherits all of the limitations of claim 1 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 4 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 4 further recites "wherein executing a directive associated with the second machine readable logic further comprises discarding the second packet." The applied combination of *Shanklin* and *Vaidya* fails to teach or suggest this further element of claim 4. The Final Office Action relies upon col. 3, lines 55-65 and col. 4, lines 54-61 of *Shanklin* as disclosing this further element of discarding the second packet, *see* page 4 of the Final Office Action. However, the cited portions of *Shanklin* merely mention that upon detecting an intrusion a connection may be terminated. There is no mention at all of discarding a second packet that is generated in response to reception of a first packet. Thus, the Final Office Action fails to establish that the combination of *Shanklin* and *Vaidya* teaches or suggests this further element of claim 4.

Accordingly, for this further reason the rejection of claim 4 should be overturned.

Dependent Claim 5

Dependent claim 5 depends from claim 4, and thus inherits all of the limitations of claim 4 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 5 is allowable at least because of its dependence from claim 4 for the reasons discussed above.

Claim 5 further recites "wherein discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node." The applied combination of *Shanklin* and *Vaidya* fails to teach or suggest this further element of claim 5.

In rejecting this claim, the Final Office Action merely asserts (at page 4 thereof) that "the examiner believes it to be inherent that discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node because any processing done at the packet level is done in the network layer of the network stack." However, in order to properly establish a rejection based on inherency, "the Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art," M.P.E.P. § 2112, *citing Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis original). The Examiner's statement fails to establish technical reasoning to support that discarding of a packet is necessarily performed at the network layer of a network stack. The Examiner asserts that any processing of a packet must be done at the network layer of the network stack without citing any supporting disclosure in the art for such allegation. Indeed, one is left to wonder why a packet may not be discarded at some other layer, such as at an application layer. For instance, one is left to wonder why a packet might not be received at an application layer and then discarded, rather than necessarily being discarded at the network layer of a network stack. Appellant respectfully asserts that the allegation by the Examiner is inaccurate and fails to sufficiently establish that a packet that is discarded must necessarily be discarded at the network layer of a network stack.

Accordingly, for this further reason the rejection of claim 5 should be overturned.

Dependent Claim 6

Dependent claim 6 depends from claim 1, and thus inherits all of the limitations of claim 1 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 6 is allowable at least because of its dependence from claim 1 for the reasons discussed above.

Claim 6 further recites "wherein reading a second packet generated by the node in response to reception of the first packet further comprises reading a second packet generated by a network stack of an operating system of the node." The applied combination of *Shanklin* and *Vaidya* fails to teach or suggest this further element of claim 6.

As discussed above with claim 1, neither *Shanklin* nor *Vaidya* teaches or suggests reading a second packet that is generated in response to reception of a first packet, and particularly not a second packet that is generated by a network stack of an operating system. The Examiner appears to contend at pages 4-5 of the Final Office Action that *Shanklin* has an operating system and that a second packet must necessarily be generated by a network stack of such operating system because "the network stack is the only layer that uses packets". However, the Examiner offers no support for this allegation, and fails to explain why other layers, such as an application layer, may not generate a packet.

Accordingly, for this further reason the rejection of claim 6 should be overturned.

Independent Claim 7 and Dependent Claims 8-9 and 12-13

Independent claim 7 recites:

> A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:
> reading a first packet;
> determining a first signature of the first packet;
> comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature;
> reading a second packet generated in response to reception of the first packet;
> determining a second signature of the second packet;
> comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature; and
> identifying the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic.
> (Emphasis added).

As discussed above with claim 1, the combination of *Shanklin* and *Vaidya* fails to teach or suggest at least "identifying the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic". Indeed, as discussed above with claim 1, neither *Shanklin* nor *Vaidya* teach or suggest using, in any way, a signature that is determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion.

Accordingly, the rejection of claim 7 should be overturned.

Claims 8-9 and 12-13 each depend from independent claim 7, and are thus likewise believed to be allowable at least based on their dependency from claim 7 for the reasons discussed above. Accordingly, Appellant respectfully requests that the rejection of claims 8-9 and 12-13 also be overturned.

Dependent Claim 10

Dependent claim 10 depends indirectly from claim 7, and thus inherits all of the limitations of claim 7 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 10 is allowable at least because of its dependence from claim 7 for the reasons discussed above.

Claim 10 further recites "wherein executing a directive comprised of machine-readable instructions further comprises executing a directive that causes the processor to discard the second packet." The applied combination of *Shanklin* and *Vaidya* fails to teach or suggest this further element of claim 10. The Final Office Action relies upon col. 3, lines 55-65 and col. 4, lines 54-61 of *Shanklin* as disclosing this further element of discarding the second packet, *see* page 4 of the Final Office Action. However, the cited portions of *Shanklin* merely mention that upon detecting an intrusion a connection may be terminated. There is no mention at all of discarding a second packet that is generated in response to reception of a first packet. Thus, the Final Office Action fails to establish that the combination of *Shanklin* and *Vaidya* teaches or suggests this further element of claim 10.

Accordingly, for this further reason the rejection of claim 10 should be overturned.

Dependent Claim 11

Dependent claim 11 depends from claim 10, and thus inherits all of the limitations of claim 10 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 11 is allowable at least because of its dependence from claim 10 for the reasons discussed above.

Claim 11 further recites "wherein executing a directive that causes the processor to discard the second packet further comprises discarding a packet at a network layer of a network stack." The applied combination of *Shanklin* and *Vaidya* fails to teach or suggest this further element of claim 11.

In rejecting this claim, the Final Office Action merely asserts (at page 4 thereof) that "the examiner believes it to be inherent that discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node because any processing done at the packet level is done in the network layer of the network stack." However, in order to properly establish a rejection based on inherency, "the Examiner must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art," M.P.E.P. § 2112, *citing Ex parte Levy*, 17 U.S.P.Q.2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (emphasis original). The Examiner's statement fails to establish technical reasoning to support that discarding of a packet is necessarily performed at the network layer of a network stack. The Examiner asserts that any processing of a packet must be done at the network layer of the network stack without citing any supporting disclosure in the art for such allegation. Indeed, one is left to wonder why a packet may not be discarded at some other layer, such as at an application layer. For instance, one is left to wonder why a packet might not be received at an application layer and then discarded, rather than necessarily being discarded at the network layer of a network stack. Appellant respectfully asserts that the allegation by the Examiner is inaccurate and fails to sufficiently establish that a packet that is discarded must necessarily be discarded at the network layer of a network stack.

Accordingly, for this further reason the rejection of claim 11 should be overturned.

Independent claim 14 and Dependent Claims 16-18

Independent Claim 14 recites:

> A node of a network operable to detect an intrusion thereof, comprising:
> a central processing unit;
> a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and
> an operating system comprising a network stack comprising a protocol

> driver, a media access control driver and a network filter service provider bound to the protocol driver and the media access control driver, the network filter service provider operable to receive a first packet and to determine a first signature of the first packet and compare the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature, the network filter service provider further operable to receive a second packet generated in response to receipt of the first packet and to determine a second signature of the second packet and compare the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature, the network filter service provider operable to identify the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic. (Emphasis added).

As discussed above with claim 1, the combination of *Shanklin* and *Vaidya* fails to teach or suggest a network filter service provider that is operable to "identify the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic". Indeed, as discussed above with claim 1, neither *Shanklin* nor *Vaidya* teach or suggest using, in any way, a signature that is determined for a second packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion.

Accordingly, the rejection of claim 14 should be overturned.

Claims 16-18 each depend from independent claim 14, and are thus likewise believed to be allowable at least based on their dependency from claim 14 for the reasons discussed above. Accordingly, Appellant respectfully requests that the rejection of claims 16-18 also be overturned.

Dependent Claim 15

Dependent claim 15 depends from claim 14, and thus inherits all of the limitations of claim 14 in addition to its own supplied limitations. It is respectfully submitted that dependent claim 15 is allowable at least because of its dependence from claim 14 for the reasons discussed above.

Claim 15 further recites "wherein the processor is operable to execute a directive causing the network filter service provider to discard the second packet." The applied combination of *Shanklin* and *Vaidya* fails to teach or suggest this further element of claim 15. The Final Office Action relies upon col. 3, lines 55-65 and col. 4, lines 54-61 of *Shanklin* as disclosing this further element of discarding the second packet, *see* page 4 of the Final Office Action. However, the cited portions of *Shanklin* merely mention that upon detecting an intrusion a connection may be terminated. There is no mention at all of discarding a second packet that is generated in response to reception of a first packet. Thus, the Final Office Action fails to establish that the combination of *Shanklin* and *Vaidya* teaches or suggests this further element of claim 15.

Accordingly, for this further reason the rejection of claim 15 should be overturned.

Independent Claim 19 and Dependent Claims 20-22

Independent claim 19 recites:

> A method of detecting an intrusion at a node of a network, comprising:
> reading a response packet by the node, the response packet generated in response to reception of a first packet by the node;
> determining a signature of the response packet;
> comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature; and
> identifying the first packet as an intrusion if the signature corresponds with the machine-readable logic. (Emphasis added).

Appellant respectfully submits that neither *Shanklin* nor *Vaidya* teaches or suggests identifying a first packet received by a node as an intrusion based on a signature of a response packet to the first packet as recited by independent claim 19. Indeed, as discussed above with claim 1, neither *Shanklin* nor *Vaidya* teach or suggest using, in any way, a signature

that is determined for a response packet that is generated in response to reception of a first packet in order to identify the first packet as an intrusion. Thus, the combination of *Shanklin* and *Vaidya* fails to teach or suggest all elements of the claim.

Accordingly, the rejection of claim 19 should be overturned.

Claims 20-22 each depend from independent claim 19, and are thus likewise believed to be allowable at least based on their dependency from claim 19 for the reasons discussed above. Accordingly, Appellant respectfully requests that the rejection of claims 20-22 also be overturned.

B. Insufficient Motivation to Combine References in the Manner Applied

It is well settled that the mere fact that references can be combined or modified is not sufficient to establish a prima facie case of obviousness, *see* M.P.E.P. § 2143.01. Rather, there must have been some explicit teaching or suggestion in the art to motivate one of even ordinary skill to combine such elements so as to create the same invention. *See Arkie Lures, Inc. v. Gene Larew Tackle, Inc.*, 119 F.3d 953, 957, 43 U.S.P.Q.2d 1294 (Fed. Cir. 1997).

Here, no such motivation exists to combine the teachings of *Vaidya* with the system of *Shanklin* in the manner suggested by the Final Office Action. The Final Office Action asserts that it would have been obvious to combine the teachings of *Vaidya* with *Shanklin* "because comparing both incoming packets to a node and outgoing packets from the same node lowers the chance of false positives because it takes two checks of the same packet (once before being acted upon and once after the packet has been received) before a packet is marked as intrusive." Pages 3-4 of the Final Office Action. Appellant fails to understand the assertion by the Final Office Action. First, comparing a signature of a first received packet with first machine readable logic and comparing a signature of a second packet that is generated in response to the first received packet with second machine readable logic does not constitute making two checks of the same packet, as asserted by the Final Office Action. Further, the Final Office Action appears to assert that double-checking the same packet to lower the chance of false positives is sufficient. This is not what is recited by the claims. Rather, a signature of packet generated in response to reception of a first packet is utilized in identifying the first packet as an intrusion, as recited in the various claims addressed above.

Thus, the relied-upon motivation is at best improper for combing the references in the manner applied, and is at worst nonsensical altogether.

Further, the asserted motivation in no way comes from the applied references themselves. That is, the relied upon references provides no motivation for making the two checks of the same packet in the manner asserted by the Office Action. A review of the references indicates that neither makes any mention of false positives, and thus the references provide no motivation for making the drastic change proffered by the Examiner in attempt to lower the chance of false positives.

In response to the above, the Final Office Action asserts:

> MPEP 2144 states that the rationale to modify or combine the prior art does not have to be expressly stated in the prior art; the rationale may be expressly or impliedly contained in the prior art or it may be reasoned from knowledge generally available to one of ordinary skill in the art, established scientific principles, or legal precedent established by prior case law.

However, no such express or implied disclosure of the Examiner's rationale in the prior art has been identified in the Final Office Action. Further, no identification of knowledge in the art, established scientific principles, or legal precedent for supporting the Examiner's rationale is identified in the Final Office Action. Thus, after stating what MPEP 2144 permits as support for the rationale for modifying the references, the Examiner fails to identify any such support for the rationale.

Further, the language of the recited motivation appears to be circular in nature, merely stating that it is obvious to make the modification because it is obvious to achieve the result. That is, the recited motivation merely states that it is obvious to perform the double-checking so that the packets will be double-checked to reduce the chances of false positives. Such language is merely a statement that the *Shanklin* reference can be modified, and does not state any desirability for making the modification. The mere fact that references can be combined or modified does not render the resultant combination or modification obvious unless the prior art also suggests the desirability of the combination or modification. *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990), as cited in M.P.E.P. § 2143.01. Thus, the motivation provided by the Examiner is improper, as the cited prior art reference must establish the desirability for making the modification.

For this further reason, the above rejections of claims 1-22 should be withdrawn.

Conclusion

In view of the above, Appellant requests that the board overturn the outstanding rejections of claims 1-22. Attached hereto are a Claims Appendix, Evidence Appendix, and Related Proceedings Appendix. As noted in the attached Evidence Appendix, no evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted. Also, as noted by the Related Proceedings Appendix, no decision has been rendered in the identified related proceeding referenced in II above, and thus no copies of any such decisions in related proceedings are provided.

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail, Label No. EV 568240731US in an envelope addressed to: M/S Appeal Brief-Patents, Commissioner for Patents, Alexandria, VA 22313.

Date of Deposit: September 18, 2006

Typed Name: Gail L. Miller

Signature: Gail L. Miller

Respectfully submitted,

By: _____

Jody C. Bishop
Attorney/Agent for Applicant(s)
Reg. No. 44,034
Date: September 18, 2006
Telephone No. (214) 855-8007

VIII. CLAIMS APPENDIX

Claims Involved in the Appeal of Application Serial No. 10/003,815

1. A method of detecting an intrusion at a node of a network, comprising:

reading a first packet received by the node;

determining a first signature of the first packet;

comparing the first signature with a signature file comprising a first machine-readable logic representative of a first packet signature;

reading a second packet generated by the node in response to reception of the first packet;

determining a second signature of the second packet;

comparing the second signature with the signature file further comprising a second machine-readable logic representative of second packet signature; and

identifying the first packet as an intrusion if the first signature corresponds with the first machine readable logic and the second signature corresponds with the second machine readable logic.

2. The method according to claim 1, further comprising executing a directive associated with the first machine readable logic upon determining the first signature corresponds with the first machine readable logic.

3. The method according to claim 1, further comprising executing a directive associated with the second machine readable logic upon determining the second signature corresponds with the second machine readable logic.

4. The method according to claim 3, wherein executing a directive associated with the second machine readable logic further comprises discarding the second packet.

5. The method according to claim 4, wherein discarding the second packet further comprises discarding the packet at the network layer of the network stack of the node.

6. The method according to claim 1, wherein reading a second packet generated by the node in response to reception of the first packet further comprises reading a second packet generated by a network stack of an operating system of the node.

7. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of:

reading a first packet;

determining a first signature of the first packet;

comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature;

reading a second packet generated in response to reception of the first packet;

determining a second signature of the second packet;

comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature; and

identifying the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic.

8. The computer-readable medium according to claim 7, further comprising an instruction set that, when executed by the processor, causes the processor to perform the computer method of executing, upon determining the first signature corresponds with the first instruction set, a directive comprised of machine-readable instructions, the first instruction set comprising the directive.

9. The computer-readable medium according to claim 7, further comprising an instruction set that, when executed by the processor, causes the processor to perform the computer method of executing, upon determining the second signature corresponds with the second instruction set, a directive comprised of machine-readable instructions, the second instruction set comprising the directive.

10. The computer-readable medium according to claim 9, wherein executing a directive comprised of machine-readable instructions further comprises executing a directive that causes the processor to discard the second packet.

11. The computer-readable medium according to claim 10, wherein executing a directive that causes the processor to discard the second packet further comprises discarding a packet at a network layer of a network stack.

12. The computer-readable medium according to claim 7, wherein comparing the first signature with a first instruction set comprising a first set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the first signature and the first set of machine readable logic.

13. The computer-readable medium according to claim 7, wherein comparing the second signature with a second instruction set comprising a second set of machine readable logic representative of a packet signature further comprises performing a binary pattern comparison with the second signature and the second set of machine readable logic.

14. A node of a network operable to detect an intrusion thereof, comprising:

a central processing unit;

a memory module for storing data in machine readable format for retrieval and execution by a central processing unit; and

an operating system comprising a network stack comprising a protocol driver, a media access control driver and a network filter service provider bound to the protocol driver and the media access control driver, the network filter service provider operable to receive a first packet and to determine a first signature of the first packet and compare the first signature with a first instruction set comprising a first set of machine readable logic representative of a first packet signature, the network filter service provider further operable to receive a second packet generated in response to receipt of the first packet and to determine a second signature of the second packet and compare the second signature with a second instruction set comprising a second set of machine readable logic representative of a second packet signature, the network filter service provider operable to identify the first packet as an intrusion if the first signature corresponds with the first set of machine readable logic and the second signature corresponds with the second set of machine readable logic.

15. The node according to claim 14, wherein the processor is operable to execute a directive causing the network filter service provider to discard the second packet.

16. The node according to claim 14, wherein the first packet is received by the node and the second packet is generated by the node.

17. The node according to claim 14, wherein the first packet is generated by the node and the second packet is received by the node.

18. The node according to claim 14, wherein the network filter service provider further comprises a pattern matching algorithm, the comparison of the first signature with the first instruction set and the comparison of the second signature with the second instruction set performed by the pattern matching algorithm.

19. A method of detecting an intrusion at a node of a network, comprising:

reading a response packet by the node, the response packet generated in response to reception of a first packet by the node;

determining a signature of the response packet;

comparing the signature with a signature file comprising a machine-readable logic representative of a packet signature; and

identifying the first packet as an intrusion if the signature corresponds with the machine-readable logic.

20. The method according to claim 19, wherein the response packet is received by the node.

21. The method according to claim 19, wherein the response packet is generated by the node.

22. The method according to claim 19, further comprising determining that the first packet is a probe packet upon determining the signature corresponds with the machine-readable logic.

IX. EVIDENCE APPENDIX

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

X. RELATED PROCEEDINGS APPENDIX

As noted in Section II above, copending Application No. 10/002,697 (hereinafter "the '697 application"), which is referenced as a related application in the present application, is on appeal before the Board. The same references are applied in rejecting the claims of the '697 application, and thus the issues raised in the '697 may be affected or have a bearing on the Board's decision in this appeal. The Board has not yet rendered a decision on the appeal of the '697 application, and thus no copies of any such decisions are provided herewith.

No further related proceedings are referenced in II above, and thus no copies of decisions in any further related proceedings are provided.